數學傳播 49卷3期, pp. 96-107

艾狄胥等人的一個加性數論定理
— 由模算術談起

張鎮華

1. 緣起 — 話說 1961 年

匈牙利數學家保羅·艾狄胥 (英文姓名 Paul Erdős, 匈牙利原名 Erdős Pál, 匈牙利人和華人一樣, 姓在先名在後) 出生於 1913 年, 在 1996 年以八十三歲高齡去世, 一生寫過的數學論文多達 1525 篇 (包括與 511人合寫的), 遠遠超過之前數百年來由 Leonhard Euler 所維持的紀錄, 成爲數學史上第一名。更可貴的是, 這些著作不只是數目多, 份量也很紮實, 其中有許多影響後來的發展十分深遠。有關他的傳記, 請參見柴契特 [1999] 和霍夫曼 [2001] 的書。

這篇文章要談的是他和 Ginzburg 及 Ziv [1961] 合作寫的有關加性數論的一個定理。

定理 1. (Erdős, Ginzburg and Ziv [1961]). 對於正整數 n, 任意整數列 $a_1, a_2, \ldots, a_{2n-1}$ 恆存在 n 項 $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$, 其和爲 n 的倍數。

定理中的項數 $2n-1$ 是最小可能, 也就是, 如果把它換成 $2n-2$, 定理就不對了。舉例來說, 如果 $a_1 = a_2 = \cdots = a_{n-1} = 0 < 1 = a_n = a_{n+1} = \cdots = a_{2n-2}$, 就找不到 n 項, 其和爲 n 的倍數。

本文要用模算術證明這個定理。我們準備由模算術的定義和基本性質說起。

2. 模算術的基本定義

模算術 (modular arithmetic) 或稱同餘算術, 是一種整數的算術系統, 其中數字超過某一個定值後會「捲回」到較小的數值, 稱爲模或餘數。模算術最早出現在德國數學家高斯 (Johann Carl Friedrich Gauss, 1777 年 4 月30日∼1855 年 2 月 23 日) 在 1801 年出版的《算術研究》(*Disquisitiones Arithmeticae*) 一書中。

在日常生活中, 我們每天都在使用模算數, 例如計時制度, 時鐘或手錶採用的是十二小時制。假設現在是九點, 八小時後會是五點。用一般的算術加法, 會得到 $9+8=17$, 但在十二小時制中, 超過十二小時會歸零, 所以「十七點」其實就是「五點」。同樣的道理, 如果現在是十

點, 那麼二十小時後的三十點會說是六點。小時數超過十二後會再回到一, 就是模 12 的模算術系統。

實務上, 我們把一天分爲上午和下午各十二小時。按照定義, 12 和 12 本身同餘, 也和 0 同餘, 所以十二點也可以說是零點; 但是實際上, 人們還是常用十二點。這會產生一點小小困惑, 上午十二點到底指的是何時? 按照直觀的感覺, 上午應該是 0:00, 1:00, ..., 11:00, 接下來似乎應該是 12:00。經查, 上午其實是以數字 $12, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ 依次序表示。所以, 上午 12:00 其實是在半夜; 爲免混淆, 常稱爲午夜 12:00、或子夜 12:00 或凌晨 12:00。類似的, 下午 12:00 最好稱爲中午 12:00 或正午 12:00。現在也有許多人用二十四小時制, 這些困擾就自然消失。

對於正整數 n, 兩個整數 a 和 b 在模 n 下同餘的意思是指 $a-b$ 爲 n 的倍數, 或是說 n 爲 $a-b$ 的因數, 也就是存在整數 c 滿足 $a-b=nc$, 記爲

$$a \equiv b \pmod{n}\text{。}$$

例如, 因爲 $28-7=21=7\times 3$ 是 7 的倍數, 所以 $28 \equiv 7 \pmod{7}$。

整數的加法、減法、乘法都具有封閉性, 也就是兩個整數經過這三種運算都會得到整數, 但是除法卻沒有這種特性, 而具有下面性質。

定理 2 (除法原理)**.** 對於正整數 n 及整數 a, 存在唯一的整數 q 使得

$$a = nq + r,$$

其中 $0 \le r < n$。這裡的 q 稱爲商, r 稱爲餘數。

根據除法原理, 任意整數 a 在模 n 下同餘於唯一的 $r \in \mathbb{Z}_n := \{0, 1, \ldots, n-1\}$。有時, 爲了特殊的應用, 我們會要求在除法原理的 r 滿足 $1 \le r \le n$, 有時會要求滿足 $-n/2 < r \le n/2$。

整數的同餘運算和普通運算有類似的規律。首先, 同餘是一個等價關係, 也就是, 對於正整數 n 和整數 a, b, c, 下列關係恆成立:

(ER1) $a \equiv a \pmod{n}$,

(ER2) 若 $a \equiv b \pmod{n}$, 則 $b \equiv a \pmod{n}$,

(ER3) 若 $a \equiv b \pmod{n}$ 且 $b \equiv c \pmod{n}$, 則 $a \equiv c \pmod{n}$。

(ER1) 成立是因爲 $a-a=0$ 是 n 的倍數。(ER2) 成立是因爲, 如果 $a-b$ 是 n 的倍數, 則 $b-a=-(a-b)$ 也是 n 的倍數。(ER3) 成立是因爲, 如果 $a-b$ 和 $b-c$ 都是 n 的倍數, 則 $a-c=(a-b)+(b-c)$ 也是 n 的倍數。

其次, 對於正整數 n 和非負整數 e, 若整數 a, b, c, d 滿足 $a \equiv b \pmod{n}$ 及 $c \equiv d \pmod{n}$, 則下列運算規律恆成立:

(O1) $a+c \equiv b+d \pmod n$,

(O2) $a-c \equiv b-d \pmod n$,

(O3) $ac \equiv bd \pmod n$,

(O4) $a^e \equiv b^e \pmod n$。

首先 $a-b$ 和 $c-d$ 都是 n 的倍數。(O1) 成立是因爲 $(a+c)-(b+d)=(a-b)+(c-d)$ 也是 n 的倍數。(O2) 成立是因爲 $(a-c)-(b-d)=(a-b)-(c-d)$ 也是 n 的倍數。(O3) 成立是因爲 $ac-bd=(a-b)c+b(c-d)$ 也是 n 的倍數。(O4) 成立是因爲 $a^e-b^e=(a-b)(a^{e-1}+a^{e-2}b+\cdots+ab^{e-2}+b^{e-1})$ 也是 n 的倍數。

在進入更多的數學性質之前, 讓我們看一些模算術有趣的應用。

3. 奇偶原理 — 翻轉杯子的應用

任意一個整數模 2 之後, 不是與 1 就是與 0 同餘, 與 1 同餘的稱爲奇數, 例如 $\pm1, \pm3, \pm5, \ldots$, 與 0 同餘的稱爲偶數, 例如 $0, \pm2, \pm4, \pm6, \ldots$。換句話說, 奇數就是可以表示爲 $2k+1$ 的整數, 偶數就是可以表示爲 $2k$ 的整數, 其中 k 爲整數。奇數和偶數有一些基本的運算性質:

奇數與奇數的和是偶數, 奇數與偶數的和是奇數, 偶數與偶數的和是偶數;

奇數與奇數的積是奇數, 奇數與偶數的積是偶數, 偶數與偶數的積是偶數。

用同餘的方式來寫就是:

$$1+1\equiv 0 \pmod 2,\ \ 1+0\equiv 1 \pmod 2,\ \ 0+0\equiv 0 \pmod 2;$$
$$1\times 1\equiv 1 \pmod 2,\ \ 1\times 0\equiv 0 \pmod 2,\ \ 0\times 0\equiv 0 \pmod 2。$$

寫成表格就是:

+	1	0
1	0	1
0	1	0

×	1	0
1	1	0
0	0	0

接著來看一些奇偶原理、也就是模 2 算術的應用。

例 1. 將 6 隻杯子排成一排, 一開始所有杯子的杯口都朝上, 每次操作是指將其中任意 4 隻杯子同時翻轉。請經過若干次操作, 將所有杯口全部朝下。

解析: 經過三次操作之後所有杯口都朝下 (每次將有星號的 4 隻杯子同時翻轉)。

$$\begin{array}{lllllll}
\text{初始:} & \bigcup * & \bigcup * & \bigcup * & \bigcup * & \bigcup & \bigcup \\
 & \bigcap & \bigcap * & \bigcap * & \bigcap * & \bigcup * & \bigcup \\
 & \bigcap & \bigcup * & \bigcup * & \bigcup * & \bigcap & \bigcup * \\
\text{結束:} & \bigcap & \bigcap & \bigcap & \bigcap & \bigcap & \bigcap
\end{array}$$

□

例 2. 將 7 隻杯子排成一排, 一開始所有杯子的杯口都朝上, 每次操作是指將其中任意 4 隻杯子同時翻轉。請經過若干次操作, 將所有杯口全部朝下。

解析: 這是做不到的, 理由如下所述。

用 a_i 表示第 i 時間時, 杯口朝上的杯子數, 所以在一開始的時候 $a_0 = 7$。如果第 i 時間時把 r 隻杯口朝上的杯子翻轉、同時把 $4-r$ 隻杯口朝下的杯子翻轉, 則

$$a_{i+1} = a_i - r + (4-r) = a_i + 4 - 2r, \text{ 即 } a_{i+1} \equiv a_i \pmod 2,$$

由於 a_0 是奇數, 所以任何 a_i 都是奇數, 不可能是 0, 所以不管怎樣翻轉, 都不可能讓所有杯口全部朝下。 □

習題 1. 將 n 隻杯子排成一排, 一開始所有杯子的杯口都朝上, 每次操作是指將其中任意 m 隻杯子同時翻轉。請經過若干次操作, 將所有杯口全部朝下。如果被翻轉的杯子都要連續, 則結論如何?

例 3. 將 16 隻杯子排成四行四列, 一開始對角線的 4 隻杯子的杯口都朝上, 其餘 12 隻杯子的杯口都朝下, 每次操作是指將其中某一行或某一列的 4 隻杯子同時翻轉。請經過若干次操作, 將所有杯口全部朝下。

$$\begin{array}{cccc}
\bigcup & \bigcap & \bigcap & \bigcap \\
\bigcap & \bigcup & \bigcap & \bigcap \\
\bigcap & \bigcap & \bigcup & \bigcap \\
\bigcap & \bigcap & \bigcap & \bigcup
\end{array}$$

解析: 這是做不到的, 理由如下所述。將這 16 隻杯子標號如下所示。

$$\begin{array}{cccc}
A & C & B & D \\
C & B & D & A \\
D & A & C & B \\
B & D & A & C
\end{array}$$

用 a, b, c, d 分別表示標號爲 A, B, C, D 的杯子杯口朝上的數目, 所以一開始有 $(a, b, c, d) = (1, 1, 2, 0)$。每一次操作把某一行或一列的 4 隻杯子同時翻轉, 因爲被翻轉的杯子包含四種不同標號杯子各恰好一隻, 所以 a, b, c, d 各數中, 原來是奇數的變爲偶數, 原來偶數的變爲奇數。因爲 a, b, c, d 這四個數中, 原來有兩個奇數、兩個偶數, 所以任何時刻還是保留爲兩個奇數、兩個偶數, 不可能變爲 $(a, b, c, d) = (0, 0, 0, 0)$。也就是, 永遠不可能讓所有杯口全部朝下。 □

習題 2. 將 16 隻杯子排成四行四列, 一開始對角線的 4 隻杯子中的 2 隻的杯口都朝上, 其餘 14 隻杯子的杯口都朝下, 每次操作是指將其中某一行、某一列、或某一對角線的 4 隻杯子同時翻轉。請經過若干次操作, 將所有杯口全部朝下。

$$\begin{array}{cccc} \cup & \cap & \cap & \cap \\ \cap & \cup & \cap & \cap \\ \cap & \cap & \cap & \cap \\ \cap & \cap & \cap & \cap \end{array}$$

4. 模算術再應用 — 骨牌在拼盤上的排列

一個 n 格骨牌是用 n 個單位正方形合成的連通圖形, 圖 1 是所有的一格骨牌、二格骨牌、三格骨牌、四格骨牌。

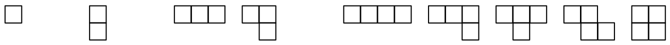

圖 1: 1 種一格骨牌、1 種二格骨牌、2 種三格骨牌、5 種四格骨牌。

小心排列, 可以發現五格骨牌共有 12 種。而六格骨牌很快就增加到 35 種。一般來說, n格骨牌隨著 n 的增加而快速增多, 要很有系統並且很小心才能正確將它們不重複地列出來。

市面上販售一種益智盤, 玩具有 12 個塑膠做成的五格骨牌, 及一個 6×10 拼盤, 問題是要把這 12 個五格骨牌放進 6×10 拼盤中。如果把對稱 (包括翻轉後相同) 的算作同一種, 答案就高達幾千種, 這要依賴計算機的幫忙才容易列出所有答案。

也可以考慮 5×12 拼盤、4×15 拼盤、3×20 拼盤, 但是顯然不能考慮 2×30 拼盤及1×60 拼盤。拼盤越瘦長的, 放的彈性就越小, 答案的數目就越少, 例如 3×20 拼盤, 扣除對稱就只有兩種。圖 2 顯示一些排法。

爲何沒有考慮四格骨牌的拼盤? 理由並不是因爲只有 5 種四格骨牌而使得問題太簡單, 而是根本無解。不管是考慮 4×5 拼盤或是 2×10 拼盤。將拼盤的 20 格黑白相間著色, 會有 10 個黑格、10 個白格。再把 5 種四格骨牌也各自黑白相間著色, 則會有 4 種四格骨牌各自含有 2 個黑格及 2 個白格, 但是有一個 T 形狀的四格骨牌含有 1 個黑格及 3 個白格 (也可以著成 3 個黑格及 1 個白格), 參見圖 3。

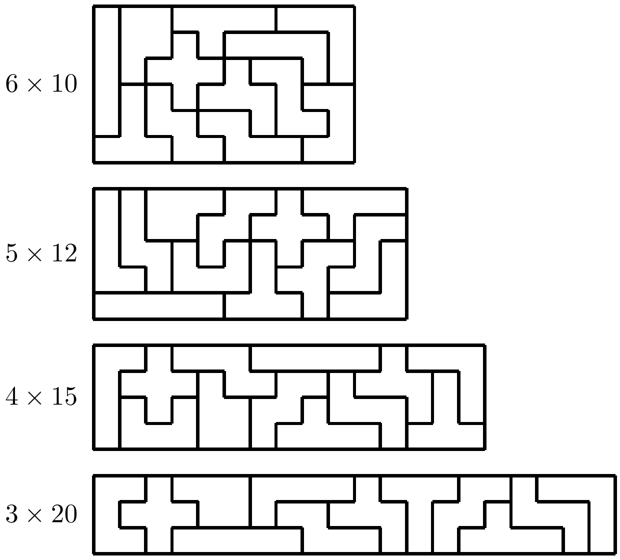

圖 2: 五格骨牌的拼盤。

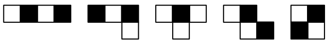

圖 3: 四格骨牌相間著色。

如果能夠將這 5 個四格骨牌拼進拼盤, 則 T 型骨牌會占用 1 個或 3 個黑格, 其他的 4 個四格骨牌各自占用 2 個黑格, 所以總共占用了 $1+2\times 4=9$ 或 $3+2\times 4=11$ 個黑格, 但這是不可能的, 因爲拼盤有 10 個黑格。

將 35 個六格骨牌放進拼盤也是做不到的, 理由類似。不管是用哪一種 $m\times n$ 拼盤, 將拼盤的 $mn=210$ 格黑白相間著色, 會有 105 個黑格、105 個白格。

再把 35 種六格骨牌也各自黑白相間著色, 則會有 24 種六格骨牌各自含有 3 個黑格及 3 個白格, 稱爲奇六格骨牌, 如圖 4 所示。

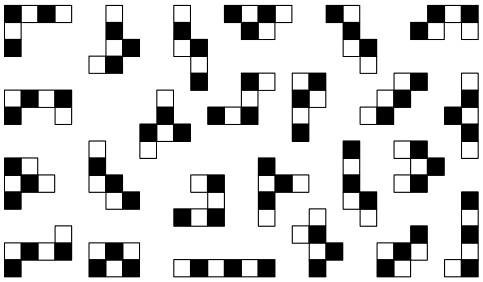

圖 4: 24 種奇六格骨牌。

另有 11 種六格骨牌各自含有 2 個黑格及 4 個白格 (也可以著成 4 個黑格及 2 個白格), 稱爲偶六格骨牌, 如圖 5 所示。

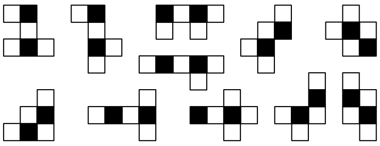

圖 5: 11 種偶六格骨牌。

如果能夠將這 35 個六格骨牌放進拼盤, 則 24 個奇六格骨牌各占用 3 個黑格, 11 個偶六格骨牌各占用 2 個或 4 個黑格, 假設有 a 個占用 2 個黑格、$11-a$ 個占用 4 個黑格, 所以總共占用了 $24\times 3+a\times 2+(11-a)\times 4=116-2a$ 個黑格, 這個數是一個偶數, 不可能等於拼盤所有的黑格數 105。

一個可能不是很容易的問題如下。

問題 1. 共有多少種七格骨牌? 所有這些七格骨牌能不能放進一個長方形拼盤?

我們之所以只問七格骨牌, 是因為, 從八格骨牌開始, 就存在有洞的骨牌。

下面來談一個利用模 3 解決問題的例子。考慮一個 8×8 拼盤 (一般常稱為西洋棋盤)。大家熟知的問題是:

(C1) 可以將 16 個二格骨牌放入 8×8 拼盤 ,

(C2) 可以將 15 個二格骨牌放入去掉兩個相鄰角的 8×8 拼盤 ,

(C3) 不可能將 15 個二格骨牌放入去掉兩個對角的 8×8 拼盤 (可用模 2 論述證明)。

現在考慮長條形三格骨牌 L。因為 $64=21\times 3+1$, 我們只能問「能不能將 21 個 L 放入 8×8 拼盤?」當然最後會剩下一格沒被骨牌覆蓋到。答案是可以的, 如圖 6 所示, 其中 $(3,3)$ 位置的方格未被覆蓋。

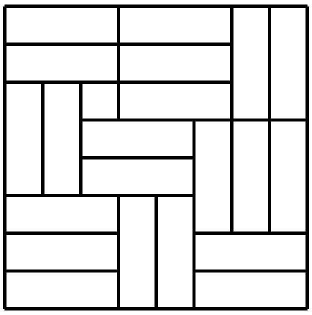

圖 6: 將 21 個 L 放入 8×8 拼盤。

如果現在把問題改為「能不能將 21 個 L 放入 8×8 拼盤, 使得被指定的某一方格 (a,b) 未被覆蓋?」前面已經給出了 $(a,b)=(3,3)$ 的答案, 對稱來說 (a,b) 為 $(3,5)$、$(5,3)$ 或 $(5,5)$ 也會有答案。那麼, 除了這四種情況以外的 (a,b) 要如何解呢? 答案是, 那就不可能了! 這要用

到模 3 來協助論證。

將 8×8 拼盤用兩種方法著三色, 分別以 $0, 1, 2$ 表示。

圖 7 左是第一種方法。著色的方法是由 $(1, 1)$ 的位置開始, 由左往右、由上往下, 循環著 $0, 1, 2$。

圖 7 右是第二種方法。著色的方法是由 $(1, 8)$ 的位置開始, 由右往左、由上往下, 循環著 $0, 1, 2$。

0	1	2	0	1	2	0	1
1	2	0	1	2	0	1	2
2	0	1	2	0	1	2	0
0	1	2	0	1	2	0	1
1	2	0	1	2	0	1	2
2	0	1	2	0	1	2	0
0	1	2	0	1	2	0	1
1	2	0	1	2	0	1	2

1	0	2	1	0	2	1	0
2	1	0	2	1	0	2	1
0	2	1	0	2	1	0	2
1	0	2	1	0	2	1	0
2	1	0	2	1	0	2	1
0	2	1	0	2	1	0	2
1	0	2	1	0	2	1	0
2	1	0	2	1	0	2	1

圖 7: 8×8 拼盤的兩種 3 著色方法。

不管是哪一種著色法, 有 21 格著 0、22 格著 1、21 格著 2。將 21 個 L 放入拼盤, 每一個都占用了著 0 的一格、著 1 的一格、著 2 的一格, 所以最後會剩下著 1 的一格未被覆蓋; 而這一格, 不管是在圖 7 左還是圖 7 右都要著 1, 那就只有可能是在 $(3, 3), (3, 5), (5, 3)$ 或 $(5, 5)$ 中的一格。

一般可以考慮下面的問題。

問題 2. 如果要將最多可能數目的長條形三格骨牌放入一般的 $m \times n$ 拼盤, 答案爲何? 如果要將最多可能數目的某一種 k 格骨牌放入一般的 $m \times n$ 拼盤, 答案爲何?

5. 從費馬小定理到歐拉公式

在整數中, 如同減法是加法的反運算, 除法是乘法的反運算。不同的是, 整數減整數得到整數, 但是整數除以整數, 有時候會得到整數, 但是有時候不一定得到整數, 也就是在除法原理中餘數 r 不爲 0 的時候, 這和把一個整數分解成整數相乘有關。

考慮一個大於 1 的正整數 n, 有一種可能是它不能被分解成兩個比它小 (因此都大於 1) 的正整數的乘積, 這時候我們把它叫做一個質數。如果 n 不是質數, 我們就可以把它分解成兩個比它小 (因此都大於 1) 的正整數的乘積 $n = ab$, 其中 $1 < a, b < n$; 如果 a 或 b 不是質數, 可以繼續把它分解成兩個比它小 (因此都大於 1) 的正整數的乘積; 繼續下去, 到頭來可以把 n 分解成一些質數的乘積。

命題 1 (質因數分解)**.** 大於 1 的正整數都可以分解成一些質數的乘積。也可以說, 大於 1 的正整數都有質因數。

舉例來說, $2100 = 2\times 2\times 3\times 5\times 5\times 7$。直觀來看, 這樣的分解應該只有一種方法, 但是要說明清楚其實是要費一些力氣的。其實, 的確有一些整數環並不是唯一分解的, 舉例來說, 若 $\mathbb{Z}$ 表示所有整數的集合, 則

$$\mathbb{Z}[\sqrt{-5}] := \{m + n\sqrt{-5} : m, n \in \mathbb{Z}\}$$

就不具有唯一分解的性質, 例如

$$6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})。$$

大於 1 的正整數可以唯一分解成質數乘積, 其關鍵是下面這個性質。

命題 2. 如果兩個正整數 a 和 b 的乘積 ab 是質數 p 的倍數, 則 a 是 p 的倍數或者 b 是 p 的倍數。也就是, 若 $ab\equiv 0 \pmod p$, 則 $a\equiv 0 \pmod p$ 或 $b\equiv 0 \pmod p$。

證明: 選取最小正整數 m 使得 am 是 p 的倍數。如果 $m=1$, 則 a 是 p 的倍數, 性質得證。所以假設 $m\geq 2$。根據除法原理

$$b = mq + r,\ 其中\ q\ 和\ r\ 都是整數、而且\ 0\leq r < m。$$

如果 $r>0$, 則因爲 $ar = a(b-mq) = ab - amq$ 也是 p 的倍數, 這和 m 的最小性矛盾, 所以事實上 $r=0$, 也就是 $b=mq$。

因爲 ap 是 p 的倍數, 和上面的論述一樣 (以 p 代替 b 的位置), 就有 $p=mq'$。但因爲 $2\leq m\leq p$、而 p 是質數, 所以 $m=p$。從而 $b=mq=pq$, 也就是 b 是 p 的倍數。 □

有了這樣的性質, 就會有正整數的唯一分解定理。

定理 3 (算術基本定理)**.** 大於 1 的正整數 n 都可以唯一分解成一些質數的乘積。也就是, n 可以分解成質數的乘積 $p_1p_2\cdots p_r$。而且, 如果 $n = p_1p_2\cdots p_r = q_1q_2\cdots q_s$, 其中 $p_1\leq p_2\leq\cdots\leq p_r, q_1\leq q_2\leq\cdots\leq q_s$ 是質數, 則 $r=s$ 且對 $1\leq i\leq r$ 恆有 $p_i=q_i$; 或是, 如果 $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} = q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s}$, 其中 $p_1<p_2<\cdots<p_r, q_1<q_2<\cdots<q_s$ 是質數, 且 $a_1,a_2,\ldots,a_r,b_1,b_2,\ldots,b_s$ 是正整數, 則 $r=s$ 且對 $1\leq i\leq r$ 恆有 $p_i=q_i$ 及 $a_i=b_i$。

證明: 由質因數分解性質知道 n 可以分解成質數的乘積。唯一性可由數學歸納法證明。

當 $r=1$ 時, 如果 $s>1$ 則 p_1 是兩個大於 1 的整數 q_1 和 $q_2q_3\cdots q_s$ 的乘積, 矛盾, 所以 $s=1$, 因此唯一性成立。

假設 $r\geq 2$ 且 $s\geq 2$。因爲 $p_1p_2\cdots p_r$ 是 q_1 的倍數, 連續使用命題 2 得知 q_1 是某個 p_i 的因數, 但是因爲 $q_1>1$ 所以事實上 $q_1=p_i$, 就有 $q_1\geq p_1$。同理可證 $p_1\geq q_1$, 而有 $p_1=q_1$。因此 $p_2p_3\cdots p_r = q_2q_3\cdots q_s$, 由歸納法假設 $r-1=s-1$、即 $r=s$, 而且對於 $2\leq i\leq r$ 恆有 $p_i=q_i$。唯一性得證。 □

命題 2 還有一個乘法消去律的面向。這和一般整數的消去律類似:

$$\text{對於整數 } a,b,c,\text{ 若 } a\neq 0 \text{ 且 } ab=ac,\text{ 則 } b=c\text{。}$$

命題 3 (模質數消去律)**.** 對於整數 a,b,c 及質數 p, 若 $a\not\equiv 0 \pmod p$ 且 $ab\equiv ac \pmod p$, 則 $b\equiv c \pmod p$。

模質數消去律在模算術中扮演基礎的角色。先來看費馬小定理。

定理 4 (費馬小定理)**.** 若 p 爲質數且整數 a 不是 p 的倍數, 則

$$a^{p-1}-1 \text{ 是 } p \text{ 的倍數, 也就是 } a^{p-1}\equiv 1 \pmod p\text{。}$$

證明: 考慮 $\mathbb{Z}_p=\{0,1,\ldots,p-1\}$ 中的元素, 對於 $i,j\in\mathbb{Z}_p$, 若 $ai\equiv aj \pmod p$, 則由模質數消去律得知 $i\equiv j \pmod p$ 也就是 $\{(ai \bmod p): i\in\mathbb{Z}_p\}=\mathbb{Z}_p$, 其中 $(ai \bmod p)$ 表示 ai 除以 p 的餘數。因此

$$(a\cdot 1)\cdot(a\cdot 2)\cdot\cdots\cdot(a\cdot(p-1))\equiv 1\cdot 2\cdot\cdots\cdot(p-1) \pmod p$$

利用模質數消去律將 $1,2,\ldots,p-1$ 逐一消去就會有 $a^{p-1}\equiv 1 \pmod p$。 □

歐拉 φ 函數定義爲: 對於大於 1 的正整數 n

$$\varphi(n)=|\{i\in\mathbb{Z}_n:\ i \text{ 和 } n \text{ 互質。}\}|$$

例如

$$\begin{aligned}
&\varphi(1)=|\{0\}|=1, && \varphi(2)=|\{1\}|=1,\\
&\varphi(3)=|\{1,2\}|=2, && \varphi(4)=|\{1,3\}|=2,\\
&\varphi(5)=|\{1,2,3,4\}|=4, && \varphi(6)=|\{1,5\}|=2,\\
&\varphi(7)=|\{1,2,3,4,5,6\}|=6, && \varphi(8)=|\{1,3,5,7\}=4,\\
&\varphi(9)=|\{1,2,4,5,7,8\}|=6, && \varphi(10)=|\{1,3,7,9\}|=4.
\end{aligned}$$

當 p 是質數時, $\varphi(p)=p-1$。費馬小定理可以推廣到一般的模 n。首先要把模質數消去律推廣。

命題 4 (模 $\boldsymbol{n}$ 消去律)**.** 對於整數 a,b,c 及正整數 n, 若 a 和 n 互質且 $ab\equiv ac \pmod n$, 則 $b\equiv c \pmod n$。

證明: 若 $b=c$, 則性質顯然成立。不妨假設 $b>c$。

由已知可見存在整數 d 使得 $a(b-c)=nd$, 不妨假設 $a>0, d>0$。在 $a,b-c,n,d$ 的質因數分解中, 由算術基本定理可得分解的唯一性, 由於 a 和 n 互質, n 分解出來的質因數不發生在 a 分解出來的質因數中, 所以必定全部發生在 $b-c$ 分解出來的質因數中, 所以 $b-c$ 是 n 的倍數, 也就是 $b\equiv c \pmod n$。 □

定理 5 (歐拉 φ 函數定理)**.** 若 n 爲正整數且整數 a 和 n 的互質, 則

$$a^{\varphi(n)}-1 \text{ 是 } n \text{ 的倍數, 也就是 } a^{\varphi(n)} \equiv 1 \pmod n\text{。}$$

證明: 考慮 $A := \{i \in \mathbb{Z}_n : i$ 和 n 互質。$\}$ 中的元素, 對於 $i, j \in A$, 若 $ai \equiv aj \pmod n$, 則由模n消去律得知 $i \equiv j \pmod n$ 也就是 $\{(ai \bmod n) : i \in A\} = A$, 其中 $(ai \bmod p)$ 表示 ai 除以 p 的餘數。因此

$$\prod_{i\in A}(a\cdot i) \equiv \prod_{i\in A} i \pmod n$$

利用模 n 消去律將 A 中的 i 逐一消去就會有 $a^{\varphi(n)} \equiv 1 \pmod n$。 □

6. 證明 Erdős-Ginzburg-Ziv 定理

最後來證明 Erdős-Ginzburg-Ziv 定理: 對於正整數 n, 任意整數列 $a_1, a_2, \ldots, a_{2n-1}$ 恆存在 n 項 $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$, 其和爲 n 的倍數。

定理對於 $n = 1$ 顯然成立。假設 $n \geq 2$。首先討論 $n = p$ 是質數的情況。先證明一個引理。

引理 1. 若 p 爲質數, $b_1, b_2, \ldots, b_s$ 是 s 個不是 p 倍數的整數, 其中 $2 \leq s < p$ 而且 $b_1 \not\equiv b_2 \pmod p$, 則最少有 $s+1$ 個模 p 不同餘的 $\sum_{i=1}^{s} \varepsilon_i b_i$, 其中各 $\varepsilon_i = 0$ 或 1。

證明: 用歸納法證明。如果 $s = 2$, 則 $b_1, b_2, b_1 + b_2$ 模 p 不同餘 (這是因爲 $b_1 \not\equiv b_2$, $b_1 \not\equiv 0$, $b_2 \not\equiv 0$)。假設 $s \geq 3$, 而且引理對 $s-1$ 成立。

令 $c_1, c_2, \ldots, c_k$ 是所有模 p 不同餘的 $\sum_{i=1}^{s-1} \varepsilon_i b_i$。由歸納法假設 $k \geq s$。如果 $k \geq s+1$, 引理成立。現假設 $k = s < p$。

如果對 $1 \leq i \leq k$ 都存在 i_r 使得 $c_i + b_s \equiv c_{i_r} \pmod p$, 因爲 $i_r = j_r$ 時 $c_i + b_s \equiv c_{i_r} \equiv c_{j_r} \equiv c_j + b_s \pmod p$, 而有 $c_i \equiv c_j \pmod p$, 也就是 $i = j$。所以

$$\sum_{i=1}^{s}(c_i + b_s) \equiv \sum_{i=1}^{s} c_i,$$

遂有 $sb_s \equiv 0 \pmod p$, 這與 $s \not\equiv 0 \pmod p$ 及 $b_s \not\equiv 0 \pmod p$ 矛盾。

所以有某一個 $c_i + b_s$ 模 p 時不與任何 c_j 同餘。引理得證。□

回到定理的證明。不妨假設 $0 \le a_1 \le a_2 \le \cdots \le a_{2p-1} < p$。

首先, 可以假設 $a_i \ne a_{i+p-1}$ (不然的話 $a_i + a_{i+1} + \cdots + a_{i+p-1} = pa_i \equiv 0 \pmod p$), 以及 $a_1 + a_2 + \cdots + a_p \equiv c \not\equiv 0 \pmod p$, 不然定理就成立了。令 $b_i = a_{p+i} - a_{i+1}$, $1 \le i \le p-1$, 則各 $b_i \not\equiv 0 \pmod p$。此時 $-c \equiv \sum_{i=1} \varepsilon_i b_i \pmod p$, $\varepsilon_i = 0$ 或 1 有解; 這是因爲如果有兩個 b_i 模 p 不同餘時, 可由前述引理推得; 而當所有 b_i 模 p 都同餘時, $\{b_2, 2b_2, \ldots, (p-1)b_2\} = \{1, 2, \ldots, p-1\}$ 而存在某個 $1 \le j \le p-1$ 滿足 $-c = jb_2$, 此時 $-c = \sum_{i=1}^{j} b_i$。顯然

$$\sum_{i=1}^{p} a_i + \sum_{i=1}^{p-1} \varepsilon_i b_i \equiv 0 \pmod p$$

是 p 個 a_i 的和。所以定理對 $n = p$ 成立。

對於一般的 n, 只要證明, 若 $n = u$ 及 $n = v$ 時定理成立, 則 $n = uv$ 時定理也成立。

考慮 $2uv - 1$ 個整數 $a_1, a_2, \ldots, a_{2uv-1}$。因爲定理對 u 成立, 可以選取其中 u 個和爲 u 倍數的 a_i, 去掉這 u 個數並重複同樣的步驟, 如果重複了 $2v-2$ 次, 還會剩下 $2uv - 1 - (2v-2)u = 2u - 1$ 個 a_i, 所以還可以選出 u 個和爲 u 倍數的 a_i。總結來說, 存在 $2v-1$ 組 $a_1^{(i)}, a_2^{(i)}, \ldots, a_u^{(i)}$, $1 \le i \le 2v-1$ 滿足 $\sum_{j=1}^{u} a_j^{(i)} = c_i u$, $1 \le i \le 2v-1$。因爲定理對 v 成立, 所以存在 $c_{i_1}, c_{i_2}, \ldots, c_{i_v}$ 使得 $\sum_{r=1}^{v} c_{i_r} \equiv 0 \pmod v$。所以

$$\sum_{r=1}^{v} \sum_{j=1}^{u} a_j^{i_r} = u \sum_{r=1}^{v} c_{i_r} \equiv 0 \pmod{uv}。$$

所以定理成立。 □

參考文獻

1. 張鎮華。閒話尤拉的絕招。數學傳播季刊, 2(3), 42–45, 1978。
2. 張鎮華。幸福結局問題—鴿籠原理與拉姆西定理。數學傳播季刊, 28(2), 28–42, 2004。
3. 張鎮華。Paul Erdős 與組合學中的機率方法。數學傳播季刊, 42(3), 25–42, 2018。
4. 張鎮華。愛小孩的歐拉 — 兼論 108 數學課綱。數學傳播季刊, 46(2), 6–19, 2022。
5. 張鎮華。《數學男孩圓周率之旅》。中大出版中心、遠流出版事業股份有信公司, 2024。
6. P. Erdős, A. Ginzburg and A. Ziv, Theorem in the additive number theory, *Bull. Res. Council Israel*, 10 (1961), 41–43.
7. 許閎揚。使用歐拉公式來求解一些平面分割數的問題。數學傳播季刊, 45(2), 38–42, 2021。
8. 保羅·霍夫曼著, 米緒軍、章曉燕、繆衛東譯。《數字愛人: 數學奇才保羅. 艾狄胥的故事》。台灣商務印書館, 2001。
9. Martin Gardner 著, 李濤庭譯。《數學迷惘》 (*Mathematical Puzzles & Diversions*), 復漢出版社, 1971。
10. T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, Inc., New York, 1951.
11. 布魯斯·柴契特著, 曾蕙蘭譯。《不只一點瘋狂: 天才數學家艾狄胥傳奇》。先覺出版社, 1999。

—本文作者爲臺灣大學數學系名譽教授—